UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

Ingenuity 13, LLC,

Plaintiff,

v.

JOHN DOE,

Defendant.

Case No. 2:12cv-520

EXHIBIT A

DECLARATION OF PETER HANSMEIER IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO THE RULE 26(f) CONFERENCE

I, Peter Hansmeier, declare under penalty of perjury as true and correct that:

1. I am a technician at 6881 Forensics, LLC (ñ6881ò).

2. On behalf of its clients, 6881 monitors and documents Internet-based piracy of our clientsô copyrighted creative content. 6881 utilizes a system of software components conceptualized, developed, and maintained in order to collect data about unauthorized distribution of copies of copyrighted works. As a technician at 6881, I am responsible for implementing day-to-day piracy monitoring. I submit this declaration in support of Plaintiffôs Motion for Leave to Take Expedited Discovery Prior to the Rule 26(f) Conference.

3. Plaintiff and other similarly situated companies contract with 6881 to have 6881 determine whether or not copies of their works are being distributed on the Internet without their permission and to identify infringers. Plaintiffôs unique copyrighted work at issue in this case is an adult video entitled ñFive Fan Favoritesò (hereinafter ñVideoò).

Background

4. Piracy is the unauthorized copying and/or distribution of copyrighted materials. Piracy of creative works (i.e., songs and motions picture) has been a serious problem since at least as early as home audio and video tape cassette players became popular. The problem continued with the introduction of home CD and DVD players. Today, the problem persists with the ability to store digital file and of songs and motion pictures in the memory of home and/or laptop computers, and for people to distribute such file to each other over the Internet on peer-to-peer networks using file sharing software applications. An article describing aspects of piracy can be found at this web page, among others, on the Internet (September 19, 2012):

http://www.thefreelibrary.com/DVD+piracy+in+the+U.S.+becomes+an+industry-a0103403775

5. Over the past decade, the ease of creating exact digital reproductions of copyrighted albums, audiovisual works, software, photographs and other forms of media has increased dramatically. Indeed, a significant amount of content, including Plaintiffôs copyrighted file, is published exclusively in digital format, which increases the publicôs access to digital reproductions. While access to digital reproductions of copyrighted media has increased, the costs of digital storage capacity and Internet bandwidth have fallen precipitously. The combination of increased access to digital content and the lower costs of storage and transmission of that content over the Internet have created a situation ripe for systemic Internet-based content piracy.

6. A development that heralded the arrival of wide scale Internet-based piracy was the introduction of modern peer-to-peer file transfer protocols. Under earlier file transfer protocols, users downloaded data directly from a central server. The rate of data transmission provided by a central server would slow dramatically when the large numbers of users requested

data simultaneously. Moreover, central servers that distributed pirated content were vulnerable to legal injunctions.

7. Modern peer-to-peer file transfer protocols substantially avoid these problems by allowing each data-seeking user to both upload to and download from other data-seeking users without the material assistance of a robust central server. In contrast to traditional file transfer protocols, modern peer-to-peer protocols actually work *better* when large numbers of users request data simultaneously because as the number of users seeking a file grows, so too does the number of users from which to download the file. Moreover, a distributed web of users is far more difficult to shut down than a central server.

8. The most popular modern peer-to-peer file transfer protocol is the BitTorrent protocol. Studies have estimated that the BitTorrent protocol accounts for up to 70% of all peer-to-peer traffic and as much as 50% of all Internet traffic in some parts of the world. Depending on the particular BitTorrent network involved, at any one time any number of people, from one or two, to several thousands, unlawfully use the BitTorrent network to upload and download copyrighted material. The premise of BitTorrent sharing is well known, and is described in length on the Bittorent.com website (last visited September 19, 2012):

http://www.bittorrent.com/help/guides/beginners-guide.

9. In BitTorrent vernacular, individual downloaders of a file are called ñpeers.ò The aggregate group of peers involved in downloading a particular file is called a ñswarm.ò A server that stores a list of peers in a swarm is called a ñtracker.ò A computer program that implements the BitTorrent protocol is called a ñBitTorrent client.ò The person who possesses a complete digital reproduction of a given file and intentionally elects to share the file with other Internet users is called the ñseeder.ò That complete file is called a ñseed.ò

10. Normal commercial computers do not come pre-loaded with the BitTorrent software. Each peer within a swarm must have separately installed on their respective computers special software that allows peer-to-peer sharing of files by way of the Internet. The seeder and peers in the swarm use software known as BitTorrent clients. Among the most popular BitTorrent clients are Vuze (formerly Azureus), εTorrent, Transmission and BitTorrent 7, although many others are used as well. In any event, the seeder and each peer must intentionally install a BitTorrent client onto his or her computer before that computer can be used to join a BitTorrent file sharing network.

11. The sharing of a file via the BitTorrent protocol operates as follows. First, the initial seeder creates a small ñtorrentò file that contains instructions for how to find the seed. The seeder uploads the torrent file to one or more of the many torrent-indexing sites. As Internet users come across the torrent file, they intentionally elect to load the torrent files in their BitTorrent client, which uses the instructions contained in the torrent file to locate the seed. These users now are peers in the swarm with respect to that digital reproduction. The BitTorrent protocol dictates that each peer download a random portion of the file (a ñpieceò) from the seed. After a peer has downloaded its first piece, it then shares that piece and subsequent pieces with other peers in the swarm. The effect of this protocol is that each peer is both copying and distributing copyrighted material at the same time. That is, each peer in a BitTorrent network has acted and acts in cooperation with other peers by agreeing to provide, and actually providing, an infringing reproduction of at least a substantial portion of a copyrighted work in anticipation of the other peers doing likewise. Joining a BitTorrent network is an intentional act, requiring the selection by a peer of multiple links to do so.

12. In BitTorrent networks, the infringement may continue even after the original seeder has gone completely offline, because the peers that have joined the swarm have become seeders themselves. Any BitTorrent client may be used to join a swarm. The more peers that join the swarm, the faster the rate of data transfer typically occurs because the odds of connecting to another peer improves. As time goes on, the size of the swarm varies, yet it may endure for a long period, with some swarms enduring for 6 months to well over a year depending on the popularity of the copyrighted work. Since the entire swarm began with a single seed, the initial seeder and peers have long lasting effects on the swarm. As a result, the original seed file becomes unlawfully duplicated multiple times by multiple parties. With respect to any particular swarm, the copied torrent file remains the same.

13. The BitTorrent protocol is particularly well suited to transferring large files, such as the audiovisual works produced by Plaintiff, as it allows even small computers with low bandwidth to be capable of participating in large data transfers across a peer-to-peer network. Where, as here, a content owner such as Plaintiff has not authorized this uncontrolled mass-reproduction and distribution of its content via the BitTorrent protocol, I believe that the copying and distribution of its content violates copyright laws. Because BitTorrent is a distributed protocol, there is no central server that can be targeted for purposes of stemming the tide of piracy. I believe that seeking recourse against individual content pirates is likely to be the most effective means of addressing BitTorrent-based content piracy.

Identification of John Doe in the Swarm

14. The life cycle as it relates to monitoring of Plaintiffôs copyrighted Video begins as follows. When a copyrighted work is requested to be monitored, my colleagues and I first check to ensure that a copyright registration exists for the work or is in process with the U.S. Copyright Office.

15. In this case, we confirmed that the work at issue in the above-captioned case is titled ñFive Fan Favoritesò with Copyright Registration Number: PA0001791654.

16. Once the copyright information is confirmed, 6881 uses its sophisticated and proprietary peer-to-peer network forensic software to perform exhaustive real time monitoring of the BitTorrent-based swarm involved in distributing the copyrighted file relevant to Plaintiffôs action. 6881ôs proprietary software is effective in capturing granular-level data about the activity of peers in the swarm and their infringing conduct and 6881ôs processes are designed to ensure that information gathered about all individual IP addresses in the swarm is accurate.

17. The digital files for which we search are available on peer-to-peer networks. A person making a copy available on a peer-to-peer network typically had obtained the copy from a peer-to-peer network. Whenever a digital file is located on anyoneôs computer on a peer-to-peer network, that file is available to be downloaded from that computer to a requestorôs computer. In every case that Plaintiffôs Video is available on a peer-to-peer network, it is an unauthorized distribution of that work. In this case, the peer-to-peer network on which we found unauthorized distribution of Plaintiffôs Video was a BitTorrent network.

18. The first step in the infringer-identification process is to locate a single swarm where peers are distributing the Video. I accomplished this step by using a variety of techniques to locate the torrent file sharing the name of copyrighted Video. Such files are commonly located on torrent indexing sites, but can also be found on Internet file-sharing forums and areas where

users congregate. Because a torrent file only contains directions about where to find the swarm associated with a particular item of digital content, the next step is to locate that swarm.

19. The most common means of locating the swarm is to connect to a BitTorrent tracker, which is a server that contains an updated list of peers in the swarm. A typical torrent file contains a list of multiple trackers associated with the underlying file. Other means of locating the swarm include using Distributed Hash Tables, which allow each peer to serve as a ñmini-trackerò and Peer Exchange, which allows peers to share data about other peers in the swarm without the use of a tracker. I used all three methods to locate the swarm associated with Plaintiffôs copyrighted Video.

20. After locating the swarm, I used 6881ôs proprietary forensic software to conduct an exhaustive real time ñfingerprintò of individuals in the swarm. Through this ñfingerprint,ò I can determine:

a. The time and date the infringer was found;

b. The time(s) and date(s) when a portion of the copyrighted file was downloaded successfully to the infringerôs computer;

c. The time and date the infringer was last successfully connected to BitTorrent network;

d. The Internet protocol (ñIPò) address assigned to the infringerôs computer;

e. The BitTorrent software application used by the infringer;

f. The size of the copyrighted file;

g. The percent of the file downloaded by 6881ôs software from the infringerôs computer;

h. The percent of the copyrighted file on the infringerôs computer which is available at that moment for copying by other peers; and

i. Any relevant transfer errors.

21. Although I was able to observe the Defendantôs infringing activity through this forensic software, this system does not allow me to access the Defendantôs computer(s) to obtain identifying personal information. Nor does this software allow me to upload a file onto Defendantôs computer(s) or communicate with it in any way. Due to the partially anonymous nature of the BitTorrent distribution systems used by the Defendant, the true name, street address, telephone number and email address of the Defendant are unknown to Plaintiff at this time. To the extent that persons using a peer-to-peer network identify themselves, they use ñuser namesò or ñnetwork namesò which typically are nicknames that do not disclose the true identity of the user, and do not indicate the residence or business address of the user. 6881 software can only identify the infringers by their IP address and the date and time they were detected in the swarm. Note that while 6881 detects an infringement at a particular instant, the infringer may, and likely is infringing at other times as well.

22. An IP address is a unique number that is assigned to Internet users by an Internet service provider (ñISPò) at a given date and time. An ISP generally records the time and dates that it assigns each IP address to a subscriber and maintains for a period of time a record of such an assignment to a subscriber in logs maintained by the ISP. In addition, the ISP maintains records which typically include the name, one or more addresses, one or more telephone numbers, and one or more email addresses of the subscriber. However, these records are not public and are not available to 6881 at this time. BitTorrent technology relies on the ability to identify the computers to and from which users can search and exchange files. The technology

identifies those computers by the IP address from which the computer connects to the Internet. Taking advantage of this technology and unique data associated with the copyrighted file is what allows 6881 to locate individuals pirating the Plaintiffôs copyrighted works.

23. There are two types of IP addresses: dynamic and static. A static IP address is an IP address that will be associated with a particular user as long as that user is a customer of a given Internet service provider. A dynamic IP address is an IP address that will change from time-to-time. Most consumer customers of ISPs are assigned a dynamic IP address. The reason for this is that an ISP can get by with a smaller overall pool of IP addresses if it simply assigns the next available IP address at a given time to a customer who wishes to connect to the Internet versus allocating a permanent and unique IP address to each of its users. ISPs keep logs of IP addresses, but the length of time they keep the logs can be as short as days.

24. If one knows a computerôs Internet Protocol address, one can, using publicly available reverse-lookup databases on the Internet, identify the ISP used by that computer. Using this information 6881 was able to determine that the ISP that provided the IP addresses associated with John Doe is Cox Communications.

25. After recording granular level data about every peer in the swarm, the next step is to carefully and thoroughly review the data produced by 6881ôs proprietary forensic software to determine what peers were actually involved in illegally reproducing and distributing Plaintiffôs Video. When a verified peer was located who made Plaintiffôs copyrighted Video available for distribution and reproduction via the BitTorrent protocol, I downloaded and retained both the torrent files and the actual digital reproductions being offered for distribution to verify that the digital copies being distributed in the swarm were in fact copies of the Plaintiffôs copyrighted Video. Because a file could be mislabeled, corrupt or otherwise not an actual copy of Plaintiffôs

Video, I physically downloaded the file and compared it to an actual copy of the Video to confirm that the file was a substantially-similar reproduction of the copyrighted Video.

26. Finally, I stored all of the data we collected in a central database for later use, examination and audit. 6881 uses these databases to record the name of the ISP having control of the IP address and the state (and often the city or county) associated with that IP address. 6881 has confirmed that the file obtained from the infringing individual is a copy of the copyrighted Video.

27. In this case, I personally observed John Doeôs IP address, listed in the Complaint (ECF No. 1 ¶ 4), downloading and uploading the Video in a BitTorrent swarm. Once obtaining a full version of the Video file, John Doe (then a ñseederò) shared pieces of that copyrighted Video file (i.e. ñseedò) with other individuals (i.e. ñpeersò).

The Critical Importance of Expedited Discovery

28. As explained above, Defendant is known to Plaintiffs only by the IP number the Defendant was assigned by the ISP on the date and time we observed the Defendant engaging in infringing conduct. The only party from whom Plaintiff can discover the Defendantôs actual name and address is the Defendantôs ISP: Cox Communications. Without expedited discovery of the Defendantôs ISP, Plaintiff will have no means of serving the Defendant with the complaint and summons in this case and no means to protect its creative content from ongoing infringement.

29. ISPs have different policies regarding the length of time they preserve information about what IP address was associated with a given subscriber at a given date and time. Some ISPs store this information for as little as months or even weeks before potentially permanently erasing the data they containð especially for dynamic IP addresses. Informal

requests for data preservation to ISPs can meet with varying degrees of success and are no substitute for formal discovery. If an ISP does not have to respond efficiently to a discovery request, the information in that ISPôs database may be erased forever. This makes expedited discovery of the identities associated with the IP addresses critically important in the instant action, particularly since nearly all IP addresses I observed in this case appeared to be associated with dynamic IP addresses.

30. Certain ISPs own excess IP addresses that they lease or otherwise allocate to third party ñintermediary ISPs.ò Because the lessor ISP has no contractual relationship with the intermediary ISPôs customers, the leasing ISP would be unable to identify the Defendant through reference to their user logs. In contrast, the intermediary ISP should be able to so identify.

31. The copyrighted file at the heart of this action continues to be made available for unlawful duplication and distribution via the BitTorrent protocol, in violation of Plaintiffôs rights to reproduce and distribute the copyrighted file. 6881 continues to monitor on a real time basis the unlawful duplication and distribution and to identify content pirates by the unique IP address assigned to them by their respective ISPs on the date and at the time of the infringing activity.

32. I am informed that before any discovery can be made in civil litigation, a meeting of the parties or the parties counsel must be held. However, the actual identity of the John Doe is unknown to Plaintiff, and therefore the Complaint cannot be served on him or her. Without serving the Complaint on a defendant, the pre-discovery meeting cannot be held. Therefore, Plaintiff needs early discovery from the ISPs, so that the names and addresses of the accused infringers can be obtained by Plaintiff to enable it to enforce its rights in its copyright and prevent continued infringement.

33. I declare under penalty of perjury that the forgoing is true and correct of my own personal knowledge, except for those matters stated as information and belief, and those matters I believe to be true, and if called upon to testify I can competently do so as set forth above.

Executed on September 19, 2012, in Minneapolis, MN.

_____

Peter Hansmeier